Minuta

MATERIA	Comentarios a la Estrategia Nacional de Seguridad Cibernética de Guatemala
AUTORES	Pablo Viollier, María Paz Canales
DESTINATARIO	Viceministro de Tecnologías de la Información y Comunicación
FECHA	13/12/2017

Comentario general

La Estrategia Nacional de Seguridad Cibernética de Guatemala (en adelante, "la Estrategia") parte de un diagnóstico crítico, pero totalmente pertinente, de la realidad actual de la protección de la ciberseguridad en Guatemala. Por ello no resulta sorprendente que en general el lenguaje usado a lo largo de la Estrategia es uno más bien de corte defensivo, que encuentra su centro en las "amenazas" a la seguridad en el ciberespacio más que en las "oportunidades" que la Estrategia brinda para dotar a Guatemala y sus habitantes de las herramientas para asegurar su participación en el ciberespacio en forma segura para el ejercicio de sus derechos.

La ventaja general de un enfoque basado en la garantía de condiciones para el ejercicio de derechos es que la estrategia puede diseñarse desde la prevención, la creación de capacidad y las oportunidades que el ciberespacio brinda a todos los sectores para su mayor desarrollo. Sin dejar de reconocer las amenazas que existen, y son reales como da cuenta correctamente la Estrategia, un enfoque en derechos que pueden ser ejercidos a través de la participación segura en el ciberespacio, tiene un efecto empoderador para todos los sectores y transmite un mensaje a la sociedad que la invita a sumarse a la tarea de resguardar la seguridad de ese espacio, más que a sentir temor de participar en él.

Es por ello que recomendamos respetuosamente la revisión del lenguaje a través del documento para ajustar el enfoque en dicho sentido. Sin que ello signifique una medida de alto impacto en los principios a los cuales la Estrategia adscribe, dicho ajuste sí tendría un efecto altamente positivo en términos de transmitir desde el Estado un mensaje de inclusión a los distintos actores sociales (en consistencia con la visión de enfoque multisectorial) y de invitación a ser protagonistas de un cambio de paradigma frente a la adopción de medidas de seguridad en el ciberespacio.

Un enfoque de la ciberseguridad centrado en el ejercicio de derechos deber ir más allá de lo meramente discursivo, para asegurar que en la estructura de gobernanza que se adopte se incorporen las medidas operativas para garantizar que tal enfoque en derechos se tenga en consideración a la hora de ejecución de cada uno de los ejes propuestos.

Visión, principios y objetivo

La Estrategia comparte la visión declarada por el Plan Estratégico de Seguridad de la Nación, el cual consiste en que "*Los guatemaltecos tendrán mayor nivel de conciencia sobre la importancia de la seguridad cibernética, la entiende, valora y aprovecha de manera efectiva, con un enfoque multisectorial en todos sus ámbitos*". Si bien la creación de mayor conciencia en la población es sin duda atingente a una estrategia de ciberseguridad, resultaría conveniente que la Estrategia en cuanto documento de política pública se plantee una visión más ambiciosa, que ponga como centro la defensa de los derechos fundamentales de los guatemaltecos. De esta forma, la visión declarada del documento puede hacer las veces de hoja de ruta para la consecución de los objetivos de la Estrategia, que proveerán contexto a un número de acciones y reformas legislativas que serán iluminadas por esta visión de mayor consecución del bienestar y progreso de los habitantes de la nación.

En cuanto a los principios declarados, el referido a "Responsabilidad compartida" estimamos respetuosamente que requiere una reformulación. La ciberseguridad es una responsabilidad compartida en el sentido que distintos actores cumplen roles particulares en su consecución. Sin embargo, la redacción actual es ambigua respecto del rol del Estado en dicha tarea, limitándose a declarar que no recae en un sujeto determinado. En tal sentido, sugerimos que el principio podría quedar redactado en la forma siguiente: "Se entiende que la promoción y protección de la seguridad cibernética compete en forma concertada a todos y cada uno de los actores sociales, públicos y privados, gubernamentales o no, los que deberán cooperar entre si en todo momento para la consecución de tal objetivo".

El principio referido a "Eficacia y Proporcionalidad" estimamos respetuosamente que también requiere de un complemento que haga más explícita su vinculación con la protección de derechos de las personas para poder desenvolverse en forma segura en el ciberespacio. En tal sentido, sugerimos que el principio podría quedar redactado en la forma siguiente: "Se refiere a un enfoque en las medidas que sean adecuadas para garantizar a las personas un uso seguro del ciberespacio para el ejercicio de sus derechos, enfocándose en las oportunidades que éste ofrece, a través de gestión de los riesgos que se hagan cargo de identificar, prevenir y dar respuesta proporcional a las amenazas en forma de asegurar en la mayor y más eficaz forma posible el ejercicio de derechos".

El principio de "Cooperación internacional" también se beneficiaría en nuestra respetuosa opinión de la incorporación explicita de que tal cooperación debe darse en el marco del respeto a los derechos fundamentales de los habitantes de Guatemala, en concordancia con los principios del derecho internacional de los derechos humanos a los cuales el país suscribe.

En cuanto a su objetivo planteado por la Estrategia, el objetivo no debiera ser la protección del ciberespacio, sino más bien asegurar las condiciones para que la participación de las personas en éste sea acorde con el ejercicio de sus derechos humanos. La estrategia en cambio lo define como *"Fortalecer las capacidades del Estado creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio".* Más allá de nuestra discrepancia respecto del enfoque planteado, incluso el objetivo adolece de un problema adicional, ya que al centrarse exclusivamente en la generación de capacidad estatal, parece contradictorio con el principio de Responsabilidad compartida. El objetivo declarado de la Estrategia debería ser más amplio que sólo fortalecer la capacidad del Estado incluyendo el fortalecimiento de los diversos sectores sociales. En tal sentido, sugerimos que el objetivo podría quedar redactado en la forma siguiente: "*Fortalecer las capacidades del Estado y los diversos actores sociales para crear el ambiente y las condiciones necesarias para brindar protección a las personas y el ejercicio de sus derechos en el ciberespacio".*

Eje 1. Marcos Legales

Resulta valorable que la Estrategia se proponga adecuar los instrumentos jurídicos del Sistema Nacional de Seguridad para incluir la seguridad cibernética desde una óptica de gestión de riesgos. Sin embargo, debido a la naturaleza dinámica de esta disciplina, es necesario agregar que las iniciativas de evaluación de riesgos deben ser actualizadas periódicamente en un proceso continuo.

Del mismo modo, resulta tremendamente positivo que la dictación de una ley contra la ciberdelincuencia tenga como correlato la dictación de una ley de privacidad y protección de datos. En particular, la legislación a dictarse en esta materia debiera abordar además del establecimiento de principios sustantivos de consentimiento previo informado, finalidad, proporcionalidad, legalidad y responsabilidad en la recogida y el tratamiento de datos, obligaciones específicas de información en episodios de fugas de datos personales.

En cuanto a la necesidad de desarrollar e implementar procesos ágiles para la colaboración e intercambio de información transnacional, es necesario explicitar en la Estrategia que dichos mecanismos sean limitados y proporcionados, y que procuren cumplir con fines legales precisos, a fin de cumplir con estándares internacional de derechos humanos.

En cuanto a la divulgación responsable de vulneraciones cibernéticas, el documento carece de especificidad respecto al modelo de notificación que se pondrá en efecto para lograr este objetivo. En particular, si se seguirá el modelo estadounidense de notificación, de carácter más bien voluntario, o un sistema más cercano al europeo, de notificación compulsoria. Creemos que este último es el que ofrece mejores garantías para la adecuada seguridad de las infraestructuras y los datos de las personas.

También se establece la necesidad de actualizar la legislación a través de la adhesión a la Convención sobre Ciberdelito del Consejo de Europa. Dicha adhesión debería plantearse de forma crítica, haciendo explícita la necesidad de estudiar plantear eventuales reservas al

tratado, o de adecuarlo al momento de implementación para resguardar los derechos fundamentales de las personas, en particular respecto de los aspectos procesales del tratado.

En cuanto a las materias no mencionadas por el documento, resulta necesario que este se pronuncie explícitamente sobre la necesidad de asegurar el respeto al debido proceso en la persecución de delitos informáticos. Del mismo modo, es necesario que el documento tome postura en lo relativo al respecto de los principios de necesariedad y proporcionalidad en la intervención de comunicaciones, y en lo posible, una referencia explícita a que la vigilancia masiva es incompatible con el respeto a los derechos fundamentales de la población.

En este sentido, se aconseja reorientar este eje, estableciendo como su principal objetivo el respeto y promoción de los derechos fundamentales manteniendo las medidas establecidas, como la mejora en la persecución del ciberdelito, como medidas específicas encaminadas a lograr dicho objetivo.

Eje 2. Educación

El énfasis del eje de educación está puesto en mejorar la capacidad del país para generar oferta educativa en materia de seguridad cibernética. Sin embargo, también resulta necesario que desde el Estado se proponga la creación de una cultura en torno a la seguridad cibernética que alcance a todos los miembros de la sociedad y no solo a quienes intervienen en ella de acuerdo a su ámbito profesional.

Más de la mitad de los ataques que ocurren en el ciberespacio son de carácter semántico, es decir, diseñados para aprovecharse de un error o engaño al usuario. Por lo mismo, es necesario que los funcionarios públicos y empleados privados de infraestructuras estratégicas, pero también usuarios del sistema bancario, del comercio electrónico o de los servicios en línea ofrecidos por el Estado sean debidamente capacitados para identificar, prevenir y reportar dichos ataques.

Del mismo modo, ciertos grupos vulnerables tales como niños, adultos mayores, mujeres, grupos vulnerables, comunidades indígenas, activistas o personas con discapacidad requieren campañas específicas para combatir fenómenos que los afectan, tales como el *phishing*, *ciberbullying*, acoso sexual, *grooming*, etc., y el gobierno debiera tomar un rol de liderazgo en diseñar y difundir tales campañas, sin perjuicio del apoyo del sector privado empresarial y académico.

Eje 3. Cultura y sociedad

En cuanto a los programas de concienciación, es necesario que estos se concentren en generar capacidad básicas en materia de autocuidado y prevención en el ciberespacio, tales como la capacidad de identificar correos de *phishing*, capacitación en la utilización de verificación de dos pasos en la autenticación para distintos servicios, la utilización de gestores de claves, y la práctica respaldar periódicamente la información valiosa.

Estimamos que la promoción de la implementación de la política de datos abiertos debe ir de la mano con una normativa de privacidad y protección de datos que requiera su anonimización para verificar que la apertura beneficie a los actores sociales, sin poner en riesgo los derechos de las personas a las cuales los datos puedan referirse.

Eje 4. Tecnologías de Información

Si bien este eje menciona la necesidad de coordinación entre distintos CSIRTS, es necesario que el Estado se proponga fomentar la creación de CSIRTs sectoriales, tales como los del sector privado, el sector financiero, el sector salud, el sector telecomunicaciones, servicios básicos, sociedad civil, academia, entre otros. Así como protocolos en los procesos de reporte que permitan la interoperabilidad de la información producida por cada uno de ellos a fin de que pueda ser usada con mayor eficacia y eficiencia.

En cuanto a la creación de un catálogo de infraestructuras críticas, es necesario tener en consideración el eventual nivel disímil de madurez de los distintos sectores, de forma que generar un cronograma concreto de trabajo.

La estrategia no se pronuncia sobre las tecnologías de cifrado, las que son clave para permitir a la industria, el gobierno y los usuarios resguardar de forma segura sus sistemas informáticos, archivos y comunicaciones. Por lo mismo, la estrategia debería comprometerse a promover el uso de este tipo de tecnologías y no impedir ni limitar su utilización.

Del mismo modo, la estrategia debería pronunciarse explícitamente en contra del diseño e implementación de “puertas traseras” (*backdoors*) compulsorias. En particular, porque implican, por definición, la inclusión de una vulnerabilidad informática que debilita deliberadamente la seguridad cibernética de dichas herramientas, tecnologías y servicios.

Gobernanza de la de la Seguridad Cibernética

En esta materia se integra la Estrategia al ámbito propio del Sistema Nacional de Seguridad, con aplicación en los campos de Seguridad Interior, Seguridad Exterior, Inteligencia de Estado y Gestión de Riesgos y Defensa Civil. A través de la creación de un Comité de Seguridad Cibernética, se busca asegurar la coordinación con la Secretaría Técnica del Consejo Nacional de Seguridad en materia de ciberseguridad. Tal estructura parece pertinente y conducente a que la seguridad del ciberespacio se inserte en la consideración más amplia de seguridad interior y exterior.

Ahora bien, sería recomendable que se especificara de manera más clara la forma en la cual en materia de ciberseguridad puedan participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria. Más que una facultad *ad hoc* sería relevante tal vez el diseño de un consejo consultivo de expertos académicos, técnicos y de la sociedad civil que pudieran en forma transparente ser seleccionados y convocados a emitir recomendaciones.

La institucionalidad propuesta contempla la creación de subcomités divididos en mesas temáticas para coordinar actuaciones en materia de ciberseguridad. Sin perjuicio del rol articulador del Comité de Seguridad Cibernética y del CSIRT-GT planteado, existe un valor que puedan existir instancias de intercambio directo intersectoriales, lo cual podría asegurarse a través del diseño institucional de reuniones cuatrimestrales de representantes de casa uno de los comités en conjunto con el Comité de Seguridad Cibernética.

Temas no mencionados en la Estrategia

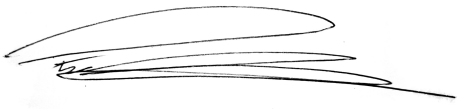
El documento no menciona la necesidad de consagrar y proteger el principio de la neutralidad de la red, el cual es clave para preservar la existencia de una internet libre, abierto e interoperativa. Incluso, en la sección de antecedentes, el documento parece valorar la existencia de planes de telefonía celular *zero-rating* como mecanismo para aumentar la cobertura de internet.

Si bien existe una preocupación por la generación de profesionales especializados en seguridad cibernética, la Estrategia no se plantea una promoción de una industria nacional de ciberseguridad, a través de la generación de demanda local para dichos servicios.

Por último, la Estrategia carece de una perspectiva de género, que le permita visibilizar y enfrentar las desigualdades que enfrentan los distintos usuarios de internet. Incluso el registro gráfico acompañado al capítulo de la construcción de la Estrategia da cuenta de la escaza participación de mujeres en los diferentes grupos de trabajo.

En concreto, mujeres y personas de sexualidad diversa son sujetos particularmente vulnerables y sometidos a tipos de amenaza específicas en el ciberespacio, normalmente en correlato a la realidad física de agresión y vulnerabilidad que les afecta. Es por ello que urge que una política de ciberseguridad tenga en particular consideración medidas que apunten a la educación de la población, la prevención y la mitigación de riesgos para asegurarles a tales sectores espacios seguros de participación en el espacio digital que les permitan confrontar las situaciones de histórica discriminación que enfrentan.

Quedamos a su disposición para aclarar o complementar cualquier aspecto relacionado con la presente minuta.



María Paz Canales
Directora Ejecutiva

Pablo Viollier
Analista de Políticas Públicas